UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,970	11/17/2003	Sundeep M. Bajikar	42.P18073	5365

45209 7590 10/28/2008

INTEL/BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
SHAN, APRIL YING	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
10/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/715,970	BAJIKAR, SUNDEEP M.	
	Examiner	Art Unit	
	APRIL Y. SHAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2008 and 11 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-6,8-13 and 15-28* is/are pending in the application.

4a) Of the above claim(s) *26-28* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-6,8-13 and 15-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/08 and 9/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The Applicant's amendment, filed 08/11/ 2008 and 4/111/08, have been received, entered into the record, and respectfully and carefully considered.

2. As a result of the amendment, claims 1, 3-6, 8-13 and 15-24 have been amended. Claims 2, 7 and 14 are canceled. Claims 25-28 are newly added claims. Claims 1, 3-6, 8-13 and 15-28 are pending.

3. Any objections/rejections not repeated below for record are withdrawn due to Applicant's amendment.

Election/Restrictions

4. Applicant's election of Species I (Claims 1, 3-6, 8-13 and 15-25), in the reply filed on 11 August, 2008 is acknowledged. However, because the Applicant did not distinctly and specifically point out the supposed errors in the restriction requirement, the election has been treated as an election without traverse (M.P.E.P 818.03(a)).

The Applicant also states non-elected Species II (Claims 26-28) has been withdrawn from consideration.

5. Claims 1, 3-6, 8-13 and 15-25 have been examined.

Terminal Disclaimer

6. The terminal disclaimer filed on 2 July 2008 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of copending Application No. 10/977,158 (U.S. Publication No. 2006/0075259) has been reviewed and is accepted. The terminal disclaimer has been recorded.

Therefore, the examiner withdraws the pending Double patenting rejection.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

9. Claims 1, 3-6, 8-13 and 15-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gehrmann et al. (U.S. Pub. No. 2004/0176071) in view of WO 01/75595 A2 (hereinafter '75595) and further in view of Le Saint et al. (U.S. Pub. No. 20040218762).

As per **claims 1 and 13**, Gehrmann et al. discloses a method/system comprising:

proving a trusted path between the application, the trusted path being a path through a trusted port of a chipset included in the computer system, wherein the trusted port is mapped to the protected section of memory ("...The subscription module further comprises an input/output **interface** 206 for communicating with the device it is inserted in..." – e.g. par. [0060], "...the communication over the **interface** provided by

the subscription module, is **protected**" – e.g. par. [0022], "...Therefore, it is an advantage of the invention that **it secures all interfaces** when providing remote access..." – e.g. par. [0061], [0037] and fig. 2. Please note protected interface and secures all interfaces correspond to Applicant's a trusted port) of a chipset (e.g. par . [0036], [0038], [0040], [0049] and [0064]-[0065]. Please note subscription module, processing means, circuit and communication means correspond to Applicant's chipset);

exchanging unencrypted data that includes an encryption key between the SIM device and the application via the trusted path ("Preferably, this key exchange may be a part of the authentication procedure. Alternatively, the key exchange is performed after successful authentication. The authentication and key exchange can be done in several different ways using well known state of art solutions...Diffie-Hellman..." – e.g. par. [0065]).,

encrypting additional data using the encryption key ("...encrypting the data using an encryption key..." – e.g. par. [0022]); and

exchanging the encrypted data between the SIM device and the application via the untrusted path (step 506 in figs. 5 and 6).

Gehrmann et al. does not explicitly disclose providing a trusted platform within a computer system for applications, the trusted platform including a protected section of memory that is inaccessible to direct memory access and an unprotected section of

memory that is accessible to direct memory access and executing an application in the trusted platform.

However, this well known feature of providing a trusted platform within a computer system for applications, the trusted platform including a protected section of memory that is inaccessible to direct memory access and an unprotected section of memory that is accessible to direct memory access and executing an application in the trusted platform is disclosed in '75595 (e.g. abstract, pages 5-8 and 16).

It would have been obvious to a person with ordinary skill in the art to combine the well known feature of '75595 with Gehrmann et al. to provide security in a computer system or platform.

Gehrmann et al. - '75595 further discloses providing an untrusted path between the application and the SIM device (Gehrmann et al., par. [0022], [0061] and fig. 3), the untrusted path being a path through untrusted port of the chipset, wherein the untrusted port is mapped to the unprotected section of memory ('75595, e.g. abstract, pages 5-8 and 16);

Gehrmann et al. - '75595 does not explicitly disclose a SIM device that includes a SIM card, the SIM device being physically connected with the computer system and wherein the unencrypted data to be exchanged is secured from unauthorized access via properties of the trusted path.

However, this well known feature of a SIM device that includes a SIM card, the SIM device being physically connected with the computer system and wherein the unencrypted data to be exchanged is secured from unauthorized access via properties

of the trusted path is disclosed in Le Saint et al. (cryptographic module 75 in fig. 1 is physically connected to a host computer system. Please further note "cryptographic module referred to…such as smart cards…SIM…" – e.g. par. [0003]. Also, in the abstract of Le Saint et al., "an SSL-like communication pathway is established between the host computer system and the cryptographic module" And SSL-like communication corresponds to Applicant's trusted path).

It would have been obvious to a person with ordinary skill in the art at the time of the invention to incorporate Le Saint et al. 's a SIM device that includes a SIM card, the SIM device being physically connected with the computer system and wherein the unencrypted data to be exchanged is secured from unauthorized access via properties of the trusted path into Gehrmann et al. - '75595 in order to enhance security by limiting an intruder's ability to intercept a cryptographic key and data.

As per **claims 3 and 15**, Gehrmann et al. further discloses wherein the exchanging the encryption key includes the application transmitting the encryption key to a protected section of memory within the computer system (e.g. paragraph [0065]); and a SIM device accessing the encryption key from the protected section of memory (e.g. paragraph [0065]).

As per **claims 4 and 16**, Gehrmann et al. further discloses wherein the exchanging the encryption key includes the application accessing the encryption key from the SIM device (e.g. paragraph [0065]), the application accessing the encryption key via the trusted port of the chipset (e.g. paragraphs [0064]-[0065]).

As per **claims 5 and 17**, Gehrmann et al. further discloses wherein the exchanging the encryption key includes exchanging multiple encryption keys ("..multiple keys…." – e.g. paragraph [0060], "a number of secret key codes K-1 through K-N…the keys may be 128 bit symmetric keys" – e.g. paragraph [0064]), and the exchanging data includes exchanging separate units of data ("…PIN codes, authorization codes, identifiers, account numbers, all messages…" – e.g. paragraph [0066]. Please note all messages such as PIN codes, account numbers corresponds to Applicant's separate units of data).

Gehrmann et al. discloses in the paragraph [0062], "the shared secret may be a secret key which is created when needed and which is valid for a specific time period, for one session, or the like, i.e. it is a temporary shared secret" and in par. [0076], "The subscription module asks…for the public key(s)…" Therefore, multiple encryption keys can be multiple encryption session keys for encrypting multiple sessions/units of data.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to encrypt each unit of data separately with an encryption key selected from the multiple encryption keys.

As per **claims 6, 8, 12, 18-20 and 24**, Gehrmann et al. further discloses wherein the exchanging data includes a host controller transmitting data from the SIM device to an unprotected section of memory ("The interfaces 304 and 306 may be implemented as plug-in interfaces…such as USB or the like…as the interfaces 304 and/or 306 of the base module are open and, thus vulnerable for unauthorized access…" – e.g.

paragraph [0061]. Please note to one with ordinary skill in the art, when using USB, there is a memory section to store USB data packets, which is vulnerable for unauthorized access as disclosed by Gehrmann et al. Therefore, it met the claim limitation of unprotected memory section disclosed by the Applicant), wherein the exchanging data includes a driver transmitting data from the unprotected section of memory to the application (e.g. paragraph [0061]), wherein the host controller is a Universal Serial Bus (USB) host controller and the driver is a USB driver (e.g. paragraph [0061]) and further including: exchanging a new encryption key based on a predetermined event selected from a group comprising of, each new transaction, passage of a predetermined period of time ("...the shared secret may be a secret key which is created when needed and which is valid for a specific time period, for one session, or the like, i.e. it is a temporary shared secret" – e.g. paragraphs [0062]) and [0068]-[0071]) and exchange of a predetermined amount of data (e.g. paragraph [0062]).

As per **claims 9 and 21**, Gehrmann et al. further discloses wherein the exchanging an encryption key includes the SIM device reading the encryption key from a protected section of memory via the trusted port of the chip set (e.g. paragraph [0064]-[0065]).

As per **claims 10 and 22**, Gehrmann et al. further discloses including: the application decrypting the encrypted data using the encryption key (e.g. paragraph [0066]).

As per **claims 11 and 23**, Gehrmann et al. – '75597 - Le Saint et al. discloses a method as applied above in claims 1 and 13. Gehrmann et al. further discloses including prior to exchanging the encryption key, the application authenticating the SIM device (e.g. paragraph [0084] and step 604 in fig. 6).

As per **claim 25**, Gehrmann et al. further discloses determining, by the SIM device, that the application is executed in the trusted platform before exchanging the unencrypted data (e.g. fig. 5 and fig. 6 and par. [0065] – [0067]. Please note only after a successful authentication and key exchange, then the data exchanging starts in the Gehrmann et al. reference).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO -892).

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to APRIL Y. SHAN whose telephone number is (571)270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/April Y Shan/
Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2431